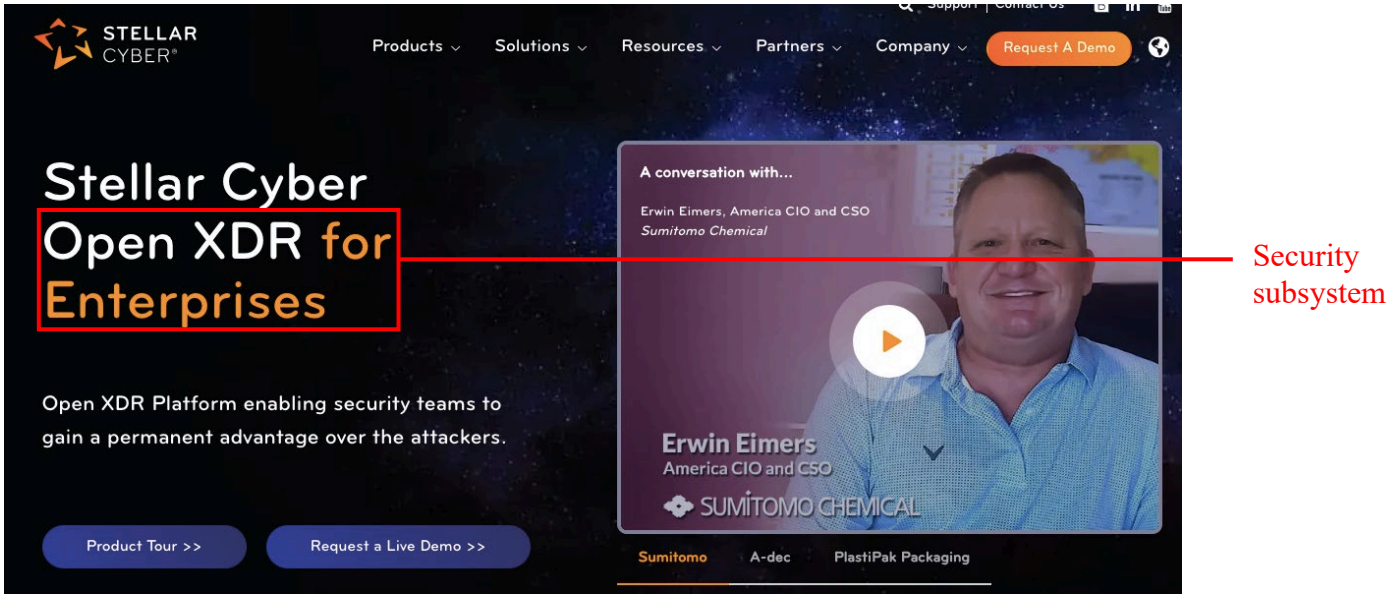
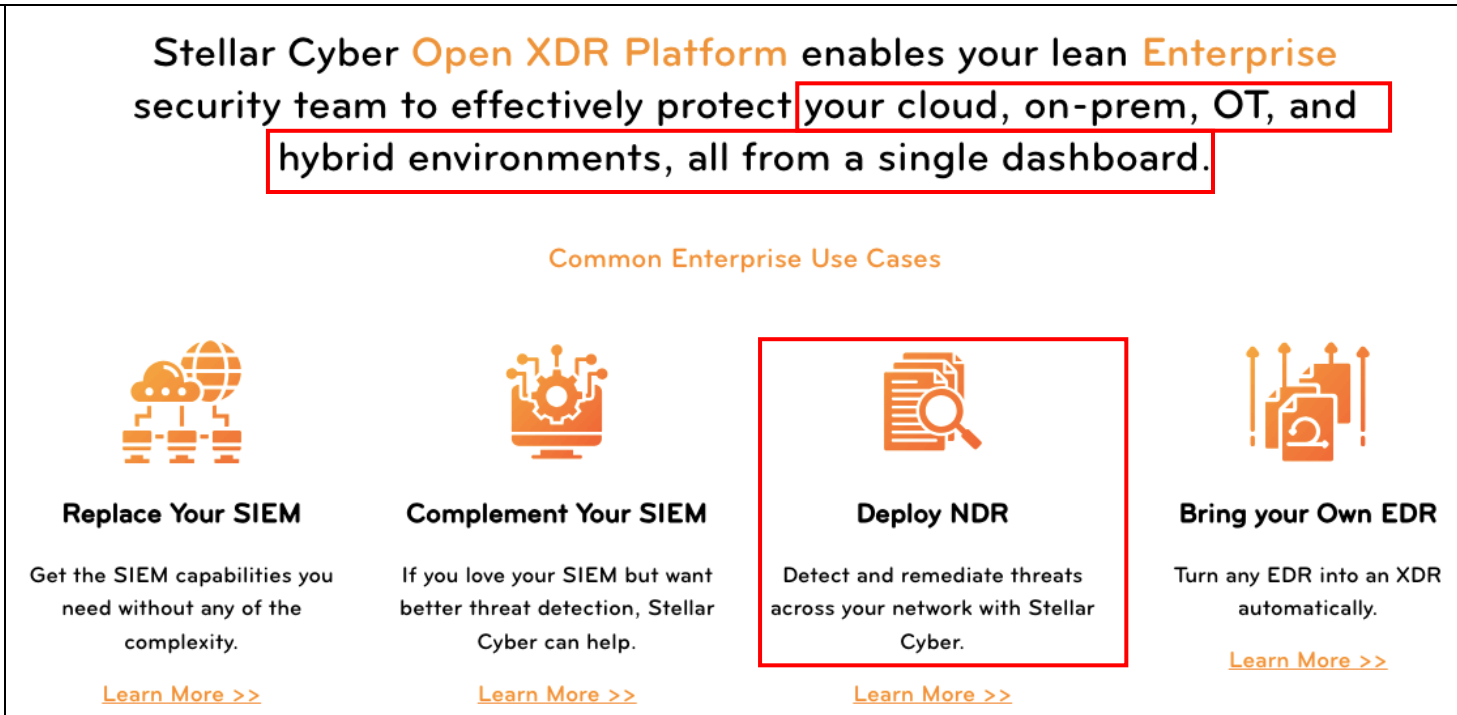
EXHIBIT B

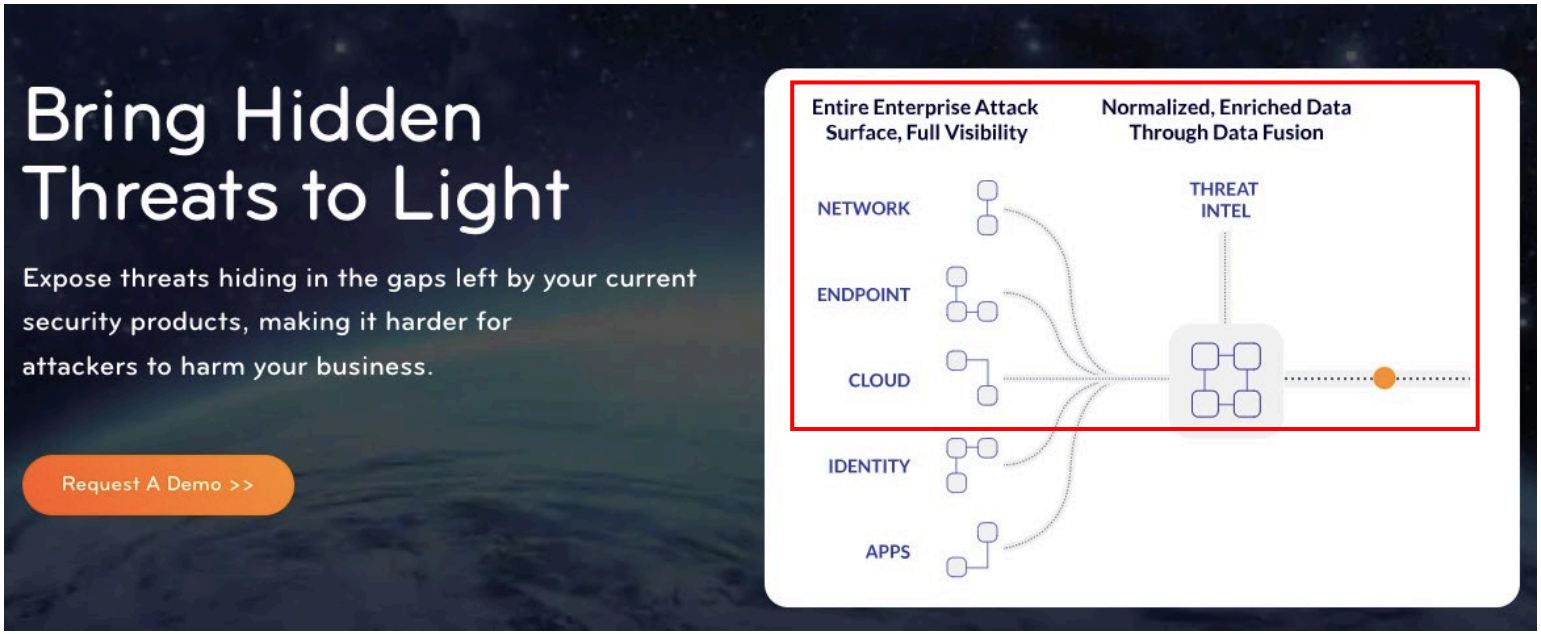
1. Claim Chart

Claim	Analysis
[14.P] A security subsystem configurable between a network and a host of an endpoint, the security subsystem comprising computing resources for providing:	Stellar Cyber ("Company") makes, uses, sells and/or offers to sell a security subsystem configurable between a network and a host of an endpoint, the security subsystem comprising computing resources. This element is infringed literally, or in the alternative, under the doctrine of equivalents. For example, Company provides Open XDR for Enterprises ("security subsystem") which includes network detection and response (NDR) that protects cloud, on-premise, OT, and hybrid environments ("configurable between a network and a host of an endpoint") from a single dashboard by detecting and remediating threats across the network. Further, it includes NexGen SIEM, TIP, UEBA, FIM, SOAR, NDR, and IDS ("computing resources") that provide security capabilities to protect IT and OT environments.  Source: https://stellarcyber.ai/product/sc-enterprises/ (annotated)



Source: https://stellarcyber.ai/product/sc-enterprises/

Source: https://stellarcyber.ai/wp-content/uploads/2023/08/08-23_OpenXDR-Datasheet.pdf, Page 1



Source: https://stellarcyber.ai/product/sc-enterprises/

Source: https://stellarcyber.ai/product/sc-enterprises/

Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Company.

[14.1] an open platform for receiving and executing security function software modules from multiple vendors for providing defense functions for protection of the host.	Company provides an open platform for receiving and executing security function software modules from multiple vendors for providing defense functions for protection of the host. This element is infringed literally, or in the alternative, under the doctrine of equivalents. For example, Company's Open XDR Platform ("open platform") integrates with third-party services ("multiple vendors") such as Acronis Cyber Protect Cloud, AWS GuardDuty, Bitdefender, and CrowdStrike Falcon to receive third-party native alerts and security events ("receiving and executing security function software modules") and create Company's alerts by applying ML/SA engines, direct mapping, and combining both the alerts, for providing security to the IT and OT environments. Stellar Cyber Open XDR Platform enables your lean Enterprise security team to effectively protect your cloud, on-prem, OT, and hybrid environments, all from a single dashboard. ‘ Source: https://stellarcyber.ai/product/sc-enterprises/ Integration of Third Party Native Alerts Stellar Cyber's built-in alerts are created from data pathways that leverage raw data collected from all forms of data sources, including third party services and Stellar Cyber's sensors. You can choose to allow Stellar Cyber's Machine Learning (ML) and Statistical Analysis (SA) to generate alerts based on raw data ingested from third party services. For certain services, you can additionally choose to ingest and integrate alerts that are natively created in *those* services. This topic summarizes which third party services and products Stellar Cyber supports for native alert integration and how those alerts are mapped in Stellar Cyber. Source: https://docs.stellarcyber.ai/prod-docs/4.3.x/Using/Alerts/Alert-Third-Party-Integration.htm

Third Party Native Alert Mapping

Stellar Cyber handles each service and product in a custom manner, according to the nature of the incoming data, including third party native alerts and other security events. To view alerts and events from multiple sources in our unified, common platform, Stellar Cyber normalizes and enriches the third party native alerts and security events during the data ingestion process. With ingested, normalized, and enriched third party native alerts and security events, Stellar Cyber further applies ML/SA engines, a direct mapping, or a combination of the two, to create Stellar Cyber alerts mapped to the XDR Kill Chain with additional de-duplication to reduce noise and alert fatigue.

Source: https://docs.stellarcyber.ai/prod-docs/4.3.x/Using/Alerts/Alert-Third-Party-Integration.htm

Third Party Service	Third Party Data Type	Ingestion Method	Mapping of Native Alerts to Stellar Cyber Alerts	Notable Interflow Fields
Acronis Cyber Protect Cloud 4.3.7	Acronis Cyber Protect Cloud Alerts	Acronis Cyber Protect Cloud Connector This connector ingests logs from Acronis Cyber Protect Cloud to get the raw alerts that are stored in the Syslog index.	Stellar Cyber maps Acronis Cyber Protect Cloud alerts. The alerts are read from the Syslog index, enriched with Stellar Cyber fields, and mapped (with de-duplication) to the Alerts index. The following four alert types are supported: Email security, EDR, Antimalware protection, and URL filtering. Tactic and Technique are based on alert type. Alerts from Acronis Email security are not correlated into cases in Case Management.	• msg_origin.source: acronis_cyber_protect • msg_class: acronis_cyber_protect_alert • Event (Alert) Name: ◦ Acronis Cyber Protect: with the assigned Technique, for example Acron Cloud: Phishing ◦ Acronis Cyber Protect: with the assigned Technique, for example Acron Cloud: XDR Anomaly ◦ Acronis Cyber Protect: with the assigned Technique, for example Acron Cloud: Hide Artifacts ◦ Acronis Cyber Protect: with the assigned Technique, for example Acron Cloud: Drive-by Compromise • Severity: Derived from event.severity_str • Fidelity: Is Severity by default • Kill Chain & MITRE | ATT&CK values are derived
AWS GuardDuty 4.3.7	AWS GuardDuty Alerts Refer to Amazon GuardDuty.	AWS GuardDuty Connector This connector ingests logs from AWS GuardDuty to get the raw alerts that are stored in the Syslog index.	Stellar Cyber maps AWS GuardDuty alerts. The alerts are read from the Syslog index, enriched with Stellar Cyber fields, and mapped (with de-duplication) to the Alerts index. Deduplication is by aws_guardduty_id.	• msg_origin.source: aws_guardduty • msg_class: aws_guardduty_finding • Event (Alert) Name: AWS GuardDuty: with the assigned Technique, for exa Valid Accounts • Severity: Derived from event.severity_str • Fidelity: Is Severity by default • Kill Chain & MITRE | ATT&CK values are derived

Multiple vendors

Source: https://docs.stellarcyber.ai/prod-docs/4.3.x/Using/Alerts/Alert-Third-Party-Integration.htm (annotated)

Bitdefender 4.3.5

URL--based

Antiphishing

Data Protection

User Control / Content Control

IP-based

Firewall

Ransomware activity detection

Threat-based

Advanced Threat Control (ATC)

Antiexploit Event

Antimalware

Hyper Detect event

Sandbox Analyzer Detection

Storage Antimalware

Configure ingestion of Bitdefender's Push event for JSON RPC messages to send data to a Stellar Cyber sensor configured to ingest httpjson (port 5200) over TLS.

Of the different record types you can configure to push to Stellar Cyber's httpjson parser, the 11 at left are normalized and enriched as they are added to the Syslog index. The records are evaluated against existing records in the Alert index-- those that do not already exist are directly mapped to the Alert index and XDR Kill chain. The other records are run through the ML/SA pipeline, which may generate alerts based on those algorithms. The labels assigned to the alert groups at left refer simply to the nature of the key data points for those alerts. Specifically, these data are supplied with the relevant alert description (Bitdefender field in parenthesis):

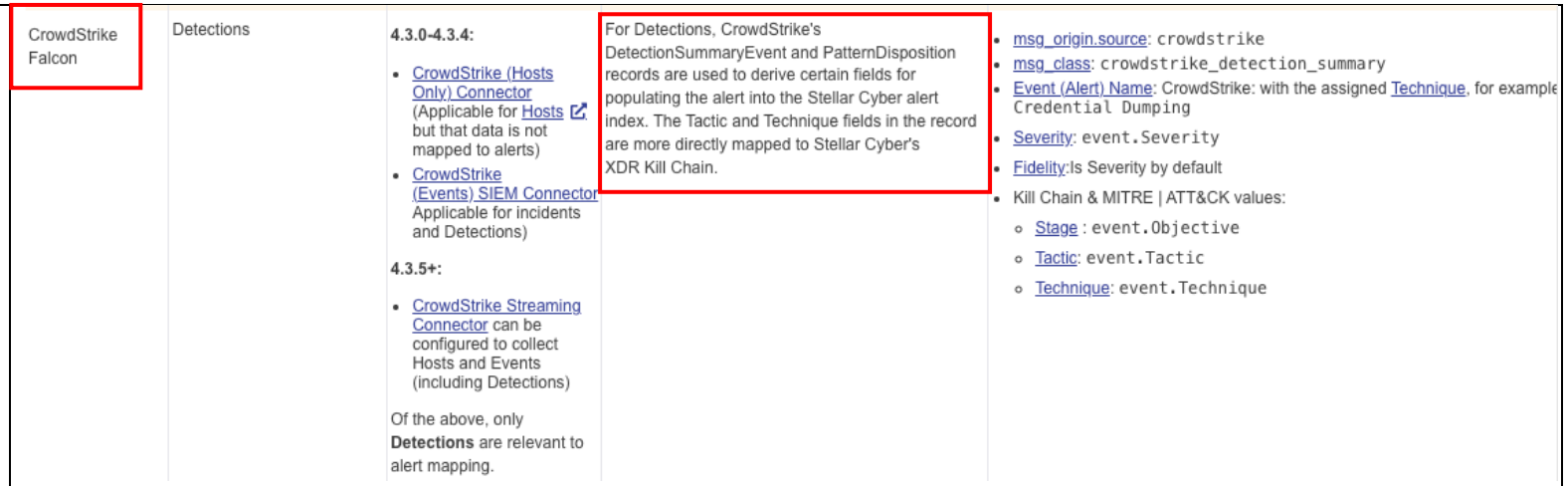
- **URL-based alerts**: event.type (module acronym), host.name (computer_fqdn), host.ip (computer_ip), url
- **IP-based alerts**: event.type (module acronym), host.name (computer_fqdn), host.ip (computer_ip), srcip (attack source or source-ip)
- **Threat-based alerts**: event.type (module acronym), host.name (computer_fqdn), host.ip (computer_ip), threatName, where threatName varies depending on the record type (malware_name, threatType, detection_threatName, attack_types, aph_type, exploit_type, or target_type)

See the Bitdefender connector information card for more details on normalization of these and other Bitdefender records.

- msg_origin.source: `bitdefender`
- msg_class: Several. See the Bitdefender connector information card for a fi
- Event (Alert) Name: Bitdefender: with the assigned Technique, for example `Encrypted for Impact`
- Severity: Derived from `event.type`
- Fidelity: Is Severity by default
- MITRE | ATT&CK Technique and Tactic values are assigned as follows:

Advanced Threat Control (ATC) Antiexploit Event Antimalware Hyper Detect event Sandbox Analyzer Detection	XDR Malware; XDR Misc Mal
User Control/Content Control	Execution; Exploitation for Cli
Data Protection Storage Antimalware Event	Impact; Data Manipulation
Ransomware activity detection	Impact; Data Encrypted for Im
Antiphishing	Initial Access; Phishing
Firewall	XDR NBA; XDR Firewall Ano

Source: https://docs.stellarcyber.ai/prod-docs/4.3.x/Using/Alerts/Alert-Third-Party-Integration.htm



	CrowdStrike Falcon	Detections	**4.3.0-4.3.4:**
			• CrowdStrike (Hosts Only) Connector (Applicable for Hosts but that data is not mapped to alerts)
			• CrowdStrike (Events) SIEM Connector Applicable for incidents and Detections)
			4.3.5+:
			• CrowdStrike Streaming Connector can be configured to collect Hosts and Events (including Detections)
			Of the above, only **Detections** are relevant to alert mapping.
				For Detections, CrowdStrike's DetectionSummaryEvent and PatternDisposition records are used to derive certain fields for populating the alert into the Stellar Cyber alert index. The Tactic and Technique fields in the record are more directly mapped to Stellar Cyber's XDR Kill Chain.	• msg_origin.source: `crowdstrike`
					• msg_class: `crowdstrike_detection_summary`
					• Event (Alert) Name: CrowdStrike: with the assigned Technique, for example `Credential Dumping`
					• Severity: `event.Severity`
					• Fidelity:Is Severity by default
					• Kill Chain & MITRE | ATT&CK values:
					  ◦ Stage : `event.Objective`
					  ◦ Tactic: `event.Tactic`
					  ◦ Technique: `event.Technique`

Source: https://docs.stellarcyber.ai/prod-docs/4.3.x/Using/Alerts/Alert-Third-Party-Integration.htm

Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Company.